Journal of Number Theory 129 (2009) 428–433

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

The large sieve inequality for integer polynomial amplitudes

Gyan Prakash, D.S. Ramana *

Harish-Chandra Research Institute, Chhatnag Road, Jhunsi, Allahabad 211 019, India

ARTICLE INFO

Article history:
Received 19 December 2007
Revised 13 May 2008
Available online 13 August 2008
Communicated by K. Soundararajan

Keywords:
Large sieve inequality
Polynomial amplitudes

ABSTRACT

We obtain a close to optimal version of the large sieve inequality with amplitudes given by the values of a polynomial with integer coefficients of degree $\geqslant 2$.

1. Introduction

It is of interest in the context of inequalities of the large sieve type to obtain estimates for the sum $\sum_{x\in\mathcal{X}} |\sum_{i\in I} a_i e(xf(i))|^2$, where $e(z)$ denotes $e^{2\pi iz}$ for any complex number z, $\mathcal{X}$ is a well-spaced sequence of real numbers, I is an interval of the integers, $\{a_i\}_{i\in I}$ are complex numbers and f is real valued function on I such that $f(I)$ is sparse, that is, the length of $f(I)$ is "much larger" than that of I. When $f(I)$ is sparse, the duality argument that is used to establish the classical large sieve inequality generally gives weak bounds thus provoking the search for alternate arguments.

Basic examples of functions f for which $f(I)$ is sparse are polynomials of degree $\geqslant 2$ and Iwaniec and Kowalski, in their book [4] (see [4, p. 184, the paragraph following Problem 7.19]), pose the question of determining good large sieve bounds when f is $P(T)$, a given polynomial in $\mathbf{Z}[T]$, and $\mathcal{X}$ is $\mathcal{F}(Q)$, the Farey sequence of order Q, where Q is a real number $\geqslant 1$. In other words, when $\mathcal{X}$ is the sequence of rational numbers $\frac{p}{q}$ with $(p,q)=1$ and $0<p\leqslant q\leqslant Q$. Our purpose here is to verify the following theorem, which provides a result in the direction of this question.

In the theorem below and thereafter $\omega(n)$ denotes the number of prime divisors of n and $\|a\|^2$ denotes $\sum_{i\in I}|a_i|^2$ for a finite sequence of complex numbers $\{a_i\}_{i\in I}$. Further, for each integer $k\geqslant 1$,

* Corresponding author.
E-mail addresses: gyan@mri.ernet.in (G. Prakash), suri@mri.ernet.in (D.S. Ramana).

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2008.05.006

we define

$$\theta(k) = k\binom{k+1}{2}. \tag{1}$$

Theorem 1. *Let Q and k be integers $\geqslant 1$ and I be an interval in $\mathbf{Z}$ of length N. When $\mathcal{F}(Q)$ is the Farey sequence of order Q and $P(T) = c_0T^k + c_1T^{k-1} + \cdots + c_k$ is a polynomial of degree k in $\mathbf{Z}[T]$ we have the inequality*

$$\sum_{x\in\mathcal{F}(Q)} \left| \sum_{i\in I} a_i e\big(xP(i)\big) \right|^2 \ll Q(N+Q)(\log 2Q)^{\omega(c_0)+\theta(k)} \|a\|^2 \tag{2}$$

for every sequence of complex numbers $\{a_i\}_{i\in I}$, where the constant implicit in the $\ll$ depends only on k.

The power of $\log 2Q$ that appears on the right-hand side of (2) is not the best that is possible even by the method of this note. In effect, we obtain this power $\log 2Q$ from bounds for the number of roots of $P(T)$ modulo m, where m is a given integer, and we have used only the simplest of such bound here (see Section 2 below).

While the classical large sieve inequality gives a much better bound than that given by (2) when $P(T)$ is linear, the bound (2) is the best possible upto the term $(\log 2Q)^{\omega(c_0)+\theta(k)}$ and constant implicit in the $\ll$ in (2) when the degree of $P(T)$ is $\geqslant 2$. We show this by means of an example in Section 3, where we provide a proof of Theorem 1.

A number of authors (see [1,7,8]) have recently obtained upper bounds for the sum on the left-hand side of (2) from various points of view. These bounds are, however, comparable to that given by (2) only when $P(T)$ is of degree 2 and the interval I is of the form $(M, M+N]$ with $M \ll N$. In fact, the only bound in the literature for polynomials $P(T)$ of degree $\geqslant 3$ that we are aware of is due to S. Baier, who uses the method of Zhao [8] to observe that (see [1, Corollary 3 following Theorem 2]) when $P(T) = T^k$, for any integer $k \geqslant 3$, and when I is of the form $(0, N]$ then the left-hand side of (2) is $\ll_\epsilon (NQ^{2(1-1/k)} + Q^2)N^{1+\epsilon} \sup_{0<i\leqslant N} |a_i|^2$ under Hooley's hypothesis K^* in the context of Waring's problem. Baier, however, deduces this from an estimate that is valid even when the Farey series is replaced with an arbitrary well-spaced set.

When indeed $P(T)$ is of degree 2 and the interval I is of the form $(0, N]$, Ramaré's method, described in Section 5.4 of [7], gives the bound $Q(N + Qg(Q))(\log_2 2Q)^2$ for the sum on the left-hand side of (2), where $g(Q) = \exp(C \log_2 Q \log_3 Q)$. Here $\log_2 Q$ and $\log_3 Q$ denote $\log\log Q$ and $\log\log\log Q$, respectively. On the other hand, Zhao [8] gives, for the same sum, upper bounds essentially of the form $(Q(NM)^{1/2} + Q^2)(NM)^\epsilon$, for each $\epsilon > 0$ when I is of the form $(M, M+N]$, via an elegant application of the double large sieve inequality. While Ramaré's estimate is sharper than that given by Theorem 1 when N is suitably larger than Q, Zhao's estimate has the advantage of being applicable when the Farey series is replaced with an arbitrary well-spaced sequence as well.

In contrast to the aforementioned results, Theorem 1 is valid for *all* integer polynomials $P(T)$ and the bound given by this theorem is *uniform* with respect to the position of the interval I.

2. Number of zeros of $P(T)$ modulo m

Let k be an integer $\geqslant 1$ and let $P(T) = c_0T^k + c_1T^{k-1} + \cdots + c_k$ be a polynomial in $\mathbf{Z}[T]$ and, for any integer $m \geqslant 1$, let $S(m)$ be the set of congruence classes l modulo m such that $P(l) \equiv 0 \bmod m$ and let $\rho(m)$ be $\mathrm{Card}(S(m))$. Let Q be a real number $\geqslant 1$. Proposition 1 below gives for $\sum_{1\leqslant m\leqslant Q} \frac{\rho(m)}{m}$ an upper bound that is *independent* of the constant term of $P(T)$. This feature of Proposition 1 is crucial to the proof of Theorem 1.

We prove Proposition 1 via a simple argument based on the Vandermonde determinant. A subtler version of this argument, due to S. Konyagin and T. Steger, is on p. 600 of [6] and in fact, this version, as also the bound given by (2) on p. 594 of [6], may be used to improve upon the conclusion of Proposition 1, and therefore, improve upon the power of $\log 2Q$ in Theorem 1.

Let p be a prime number and m, n be integers $\geqslant 1$. When $m \geqslant n$ the image of $S(p^m)$ under the canonical surjection from $\mathbf{Z}/p^m\mathbf{Z}$ onto $\mathbf{Z}/p^n\mathbf{Z}$ is contained in $S(p^n)$. Therefore we have $\frac{\rho(p^m)}{p^m} \leqslant \frac{\rho(p^n)}{p^n}$ whenever $m \geqslant n \geqslant 1$.

Suppose now that p is a prime number that does not divide c_0. We then have $\rho(p) \leqslant k$ and hence $\frac{\rho(p^m)}{p^m} \leqslant \frac{k}{p}$ for all $m \geqslant 1$. We shall presently improve upon this upper bound for large m. To this end we set, for any integer $m \geqslant 1$, $a(m,k)$ to denote the smallest integer $\geqslant \frac{m}{\binom{k+1}{2}}$. We shall verify that any interval of the real line of length $p^{a(m,k)}$ contains no more than $k+1$ integers x such that $P(x)$ is divisible by p^m. To verify this, it suffices to show that when $x_1, x_2, \ldots, x_{k+1}$ are distinct integers such that $P(x_i)$ is divisible by p^m for each i, we have $\sup_{i,j} |x_i - x_j| \geqslant p^{a(m,k)}$. Indeed, on recalling the well-known identity for the Vandermonde determinant we have

$$c_0 \prod_{1 \leqslant i < j \leqslant k+1} (x_i - x_j) = \begin{vmatrix} 1 & 1 & \ldots & 1 \\ x_1 & x_2 & \ldots & x_{k+1} \\ \vdots & \vdots & & \vdots \\ x_1^{k-1} & x_2^{k-1} & \ldots & x_{k+1}^{k-1} \\ P(x_1) & P(x_2) & \ldots & P(x_{k+1}) \end{vmatrix}. \tag{1}$$

Since the right-hand side of (1) is divisible by p^m and p does not divide c_0, we see that p^m divides $\prod_{1 \leqslant i < j \leqslant k+1} (x_i - x_j)$. Consequently,

$$\binom{k+1}{2} \sup_{i \neq j} v_p(x_i - x_j) \geqslant \sum_{1 \leqslant i < j \leqslant k+1} v_p(x_i - x_j) \geqslant m. \tag{2}$$

It follows from (2) that $\sup_{i \neq j} v_p(x_i - x_j) \geqslant a(m,k)$ and, because the x_i are distinct, that $\sup_{i,j} |x_i - x_j| \geqslant p^{a(m,k)}$.

For each integer $m \geqslant 1$, the set $S(p^m)$ is in bijection with the subset of the integers x in the interval $[0, p^m)$ such that $P(x)$ is divisible by p^m. On dividing this interval into subintervals of length $p^{a(m,k)}$ and noting that $a(m,k) \leqslant m$ for all $m \geqslant 2$, we then conclude that when p does not divide c_0 we have $\rho(p^m) \leqslant \frac{2(k+1)p^m}{p^{a(m,k)}}$, for all $m \geqslant 2$.

With the aid of the bounds for $\frac{\rho(p^m)}{p^m}$ given above we then conclude that when p is a prime number that does not divide c_0 we have

$$\sum_{m \geqslant 0} \frac{\rho(p^m)}{p^m} \leqslant 1 + \sum_{1 \leqslant m \leqslant \binom{k+1}{2}} \frac{k}{p} + \sum_{m > \binom{k+1}{2}} \frac{2(k+1)}{p^{a(m,k)}} = 1 + \frac{\theta(k)}{p} + 2(k+1)\binom{k+1}{2} \sum_{m \geqslant 2} \frac{1}{p^m}, \tag{3}$$

where the last identity follows on dividing the sum over $m > \binom{k+1}{2}$ into sums over congruence classes modulo $\binom{k+1}{2}$ and noting that $a(l + d\binom{k+1}{2}, k) = d+1$, when d is any integer and l an integer satisfying $0 < l \leqslant \binom{k+1}{2}$.

Proposition 1. *Let $P(T) = c_0 T^k + c_1 T^{k-1} + \cdots + c_k$ be a polynomial of degree $k \geqslant 1$ in $\mathbf{Z}[T]$ and let $\rho(m)$, for each integer $m \geqslant 1$, be the number of residue classes l modulo m such that $P(l) \equiv 0 \bmod m$. For any real number $Q \geqslant 1$ we then have $\sum_{1 \leqslant m \leqslant Q} \frac{\rho(m)}{m} \ll (\log 2Q)^{\omega(c_0)+\theta(k)}$, where the implied constant in the $\ll$ depends only on k.*

Proof. We may assume that $Q \geqslant 2$. In that case, since $\rho(m)$ is multiplicative, the sum $\sum_{1 \leqslant m \leqslant Q} \frac{\rho(m)}{m}$ is majorised by

$$\prod_{2\leqslant p\leqslant Q}\Bigg(\sum_{\substack{m\geqslant 0\\ p^m\leqslant Q}}\frac{\rho(p^m)}{p^m}\Bigg)\leqslant(\log 2Q)^{w(c_0)}\prod_{\substack{2\leqslant p\leqslant Q\\ p\nmid c_0}}\left(1+\frac{\theta(k)}{p}+2(k+1)\binom{k+1}{2}\sum_{m\geqslant 2}\frac{1}{p^m}\right),\tag{4}$$

where we have used the trivial bound $\rho(p^m)\leqslant p^m$ for primes p dividing c_0 and the bound given by (3) when p does not divide c_0, that is, when $\gcd(c_0,p)=1$. The proposition now follows on dropping the condition $p\nmid c_0$ in the product on the right-hand side of (4) and noting that $\prod_{2\leqslant p\leqslant Q}(1+\frac{a}{p}+b\sum_{m\geqslant 2}\frac{1}{p^m})\ll_{a,b}(\log 2Q)^a$, for any real numbers a and $b\geqslant 0$. □

3. Proof of the large sieve inequality

For each $(i,j)\in I\times I$ let us set

$$K(i,j)=\sum_{x\in\mathcal{F}(Q)}e\big(x\big(P(i)-P(j)\big)\big)\tag{1}$$

so that $|K(i,j)|=|K(j,i)|$, for each (i,j). On squaring out the sum over $i\in I$ in the left-hand side of the inequality given by Theorem 1, interchanging the summations and applying the triangle inequality together with $|a_i\bar{a_j}|\leqslant\frac{1}{2}(|a_i|^2+|a_j|^2)$ for each (i,j) we obtain

$$\sum_{x\in\mathcal{F}(Q)}\Bigg|\sum_{i\in I}a_ie\big(xP(i)\big)\Bigg|^2=\sum_{(i,j)\in I\times I}a_i\bar{a_j}K(i,j)\leqslant\|a\|^2\sup_{j\in I}\sum_{i\in I}\big|K(i,j)\big|.\tag{2}$$

We now estimate the right-hand side of (2) with the aid of the classical estimate

$$\Bigg|\sum_{\substack{0\leqslant p\leqslant q-1\\ \gcd(p,q)=1}}e\left(\frac{ap}{q}\right)\Bigg|\leqslant\gcd(a,q),\tag{3}$$

which is valid for any integer a with the convention that $(0,q)=q$. In effect, on writing $c(i,j)$ to denote $P(i)-P(j)$, for each (i,j) and using (3) we have

$$\big|K(i,j)\big|\leqslant\sum_{1\leqslant q\leqslant Q}\Bigg|\sum_{\substack{0\leqslant p\leqslant q-1\\ \gcd(p,q)=1}}e\left(\frac{pc(i,j)}{q}\right)\Bigg|\leqslant\sum_{1\leqslant q\leqslant Q}\gcd\big(c(i,j),q\big).\tag{4}$$

Since for any integer m with $1\leqslant m\leqslant Q$, the number of multiples q of m with $1\leqslant q\leqslant Q$ does not exceed $\frac{Q}{m}+1\leqslant\frac{2Q}{m}$, we obtain

$$\sum_{1\leqslant q\leqslant Q}\gcd\big(c(i,j),q\big)\leqslant\sum_{\substack{1\leqslant m\leqslant Q\\ m\mid c(i,j)}}m\sum_{\substack{1\leqslant q\leqslant Q\\ q\equiv 0\bmod m}}1\leqslant 2Q\sum_{\substack{1\leqslant m\leqslant Q\\ m\mid c(i,j)}}1.\tag{5}$$

For any $j\in I$, let us set $\rho_j(m)$ to denote the number of congruence classes l modulo m for which $P(l)\equiv P(j)\bmod m$. On combining (5) with (4) and recalling that I is an interval of length N, we then conclude that for each $j\in I$,

$$\sum_{i\in I}\big|K(i,j)\big|\leqslant 2Q\sum_{i\in I}\sum_{\substack{1\leqslant m\leqslant Q\\ m\mid c(i,j)}}1=2Q\sum_{1\leqslant m\leqslant Q}\sum_{\substack{i\in I\\ c(i,j)\equiv 0\bmod m}}1\leqslant 2Q\sum_{1\leqslant m\leqslant Q}\rho_j(m)\left(\frac{N}{m}+1\right).\tag{6}$$

On applying Proposition 1 to the polynomial $P(T) - P(j)$, we see, for each $j \in I$, that

$$\sum_{1 \leqslant m \leqslant Q} \rho_j(m)\left(\frac{N}{m} + 1\right) \leqslant \sum_{1 \leqslant m \leqslant Q} (N+Q)\frac{\rho_j(m)}{m} \ll (N+Q)(\log 2Q)^{\omega(c_0)+\theta(k)}, \tag{7}$$

which when combined with (2) and (6) gives Theorem 1.

Let us verify that upto the term $(\log 2Q)^{\omega(c_0)+\theta(k)}$ and the constant implicit in $\ll$ the bound given by Theorem 1 is the best possible. To this end, let us take $P(T) = T^k$, where $k \geqslant 2$ and define, for any integers p and q, with $q \neq 0$, $S(p,q)$ by the relation

$$S(p,q) = \sum_{1 \leqslant i \leqslant q} e\left(\frac{pP(i)}{q}\right). \tag{8}$$

We then learn on p. 24 of [5] that when q is a *prime number* we have

$$\sum_{1 \leqslant p \leqslant q-1} \left|S(p,q)\right|^2 = (k-1)q(q-1). \tag{9}$$

Moreover, we have the bound $|\sum_{1 \leqslant i \leqslant q} e(\frac{pP(i)+li}{q})| \leqslant (k-1)q^{1/2}$ from the estimate of Weil for exponential sums, for all prime numbers $q > k$ and all integers p, l with $(p,q) = 1$. On combining this bound with Theorem 2 of [5, p. 12] we then deduce that

$$\left|\sum_{1 \leqslant i \leqslant m} e\left(\frac{pP(i)}{q}\right)\right| \leqslant 2(k-1)q^{1/2}\log q, \tag{10}$$

for all prime numbers $q > k$ and all integers p, m with p and m in the interval $[1, q-1]$. In particular, we have $|S(p,q)| \leqslant 2(k-1)q^{1/2}\log q$.

Let us now take Q to be a real number $> k$ such that $\pi(Q) - \pi(k) \geqslant \frac{Q}{2\log Q}$, where, as usual, $\pi(x)$ is the prime counting function. Such a Q is provided by the Chebyshev estimate for $\pi(x)$. Let N be an integer $\geqslant 64(k-1)Q\log^2 Q$ and let q be a prime number satisfying $k < q \leqslant Q$. On dividing the interval $(0, N]$ into subintervals of length q and applying the triangle inequality together with (10) we then see that

$$\sum_{1 \leqslant p \leqslant q-1} \left|\sum_{1 \leqslant i \leqslant N} e\left(\frac{pP(i)}{q}\right)\right|^2 \geqslant \sum_{1 \leqslant p \leqslant q-1} \left(\left[\frac{N}{q}\right]\left|S(p,q)\right| - 2(k-1)q^{1/2}\log q\right)^2. \tag{11}$$

Let us set $E = 2(k-1)q^{1/2}\log q$. Then the right-hand side of (11) is the same as

$$\left[\frac{N}{q}\right]^2 \sum_{1 \leqslant p \leqslant q-1} \left|S(p,q)\right|^2 - 2\left[\frac{N}{q}\right]E \sum_{1 \leqslant p \leqslant q-1} \left|S(p,q)\right| + E^2(q-1). \tag{12}$$

Since $|S(p,q)| \leqslant E$ for all p in $[1, q-1]$, we have that $\sum_{1 \leqslant p \leqslant q-1} |S(p,q)| \leqslant qE$. Thus, on using (9) together with $N \geqslant 64(k-1)Q\log^2 Q$, $q \geqslant 1$, we deduce that the left-hand side of (11) is minorised by

$$\left[\frac{N}{q}\right]^2 \sum_{1 \leqslant p \leqslant q-1} \left|S(p,q)\right|^2 - 2\left[\frac{N}{q}\right]qE^2 \geqslant \frac{(k-1)N^2}{4} - 2NE^2 \geqslant \frac{(k-1)N^2}{8}. \tag{13}$$

On account of our choice of Q we finally conclude that

$$\sum_{x\in\mathfrak{F}(Q)}\left|\sum_{0<i\leqslant N} e\big(xP(i)\big)\right|^2 \geqslant \sum_{\substack{1\leqslant q\leqslant Q\\ q\text{ prime}\\ q>k}}\ \sum_{1\leqslant p\leqslant q-1}\left|\sum_{0<i\leqslant N} e\left(\frac{pP(i)}{q}\right)\right|^2 \geqslant \frac{(k-1)N^2Q}{16\log Q}, \tag{14}$$

which may be compared with the upper bound $\ll_k N^2 Q(\log Q)^{\theta(k)}$ for the first term on the left-hand side of (14) supplied by Theorem 1 when applied with I taken to be the interval of integers $(0, N]$, the polynomial $P(T) = T^k$ and all the $a_i = 1$. When $N < 64(k-1)Q\log^2 Q$, Theorem 1 gives the upper bound $\ll_k Q^2(\log Q)^{\theta(k)+2}\|a\|^2$ for the left-hand side of (2), which may be compared with the lower bound $Q^2\|a\|$ for this term, which is obtained when I is taken to be the interval $(0, 1]$.

The method of proof of Gallagher's inequality (see [3, p. 16] or [2, p. 144]) immediately implies the following corollary to Theorem 1.

Corollary. *Let D and k be integers $\geqslant 1$. When I is an interval of the integers of length N and $P(T) = c_0T^k + c_1T^{k-1} + \cdots + c_k$ is a polynomial of degree k in $\mathbf{Z}[T]$ we have the inequality*

$$\sum_{1\leqslant d\leqslant D}\frac{d}{\phi(d)}\sum_{\chi \bmod^* d}\left|\sum_{i\in I} a_i\chi\big(P(i)\big)\right|^2 \ll D(N+D)(\log D)^{\omega(c_0)+\theta(k)}\|a\|^2 \tag{15}$$

for every sequence of complex numbers $\{a_i\}_{i\in I}$, where the constant implicit in the $\ll$ depends only on k.

Acknowledgments

Our deepest thanks go to Professor Olivier Ramaré for generously providing us with his time and suggestions. We are indebted to Dr. Liangyi Zhao, Professor R. Balasubramanian and Professor R. Heath-Brown for discussing the problem addressed here with us.

References

[1] S. Baier, The large sieve with quadratic amplitude, Funct. Approx. 36 (2006) 33–43.
[2] A.C. Cojocaru, R. Murty, An Introduction to Sieve Methods and Their Applications, London Math. Soc. Stud. Texts, vol. 66, 2005.
[3] P.X. Gallagher, The large sieve, Matematika 14 (1967) 14–20.
[4] H. Iwaniec, E. Kowalski, Analytic Number Theory, Amer. Math. Soc. Colloq. Publ., vol. 53, 2004.
[5] N.M. Korobov, Exponential Sums and Their Applications, Kluwer Academic Publishers, 1989.
[6] S. Konyagin, T. Steger, On polynomial congruences, Math. Notes 55 (5) (1996) 596–600.
[7] O. Ramaré, Arithmetical Aspects of the Large Sieve Inequality, Hindustan Book Agency, in press.
[8] L. Zhao, Large sieve inequalities with quadratic amplitudes, Monatsh. Math. 151 (2) (2007) 165–173.